Apple lanza actualizaciones de iPhone y iPad para corregir vulnerabilidad DoS en HomeKit

Autor: I. Stepanenko

Fecha: Monday 24th of January 2022 10:18:33 AM

Apple lanzó este miércoles actualizaciones de software para iOS y iPadOS, para corregir un problema persistente de denegación de servicio (DoS), que afecta al marco del hogar inteligente HomeKit, que podría explotarse potencialmente para lanzar ataques de tipo ransomware dirigidos a los dispositivos.

La compañía, en sus notas de lanzamiento para iOS y iPadOS 15.2.1, lo calificó como un *«problema de agotamiento de recursos»,* que podría desencadenarse al procesar un nombre de accesorio de HomeKit creado con fines maliciosos, y agregó que solucionó el error con una validación mejorada.

La vulnerabilidad llamada doorLock, rastreada como CVE-2022-22588, afecta a HomeKit, la API de software para conectar dispositivos domésticos inteligentes a aplicaciones iOS.

De explotarse con éxito, los iPhones y iPads pueden caer en una espiral de choque simplemente cambiando el nombre de un dispositivo HomeKit a una cadena de más de 500,000 caracteres y engañando al objetivo para que acepte una invitación de Home

maliciosa.

Peor todavía, debido a que los nombres de los dispositivos de HomeKit están respaldados en iCloud, volver a iniciar sesión en la cuenta de iCloud afectada vinculada al dispositivo HomeKit, puede volver a desencadenar la condición DoS y hacer que los dispositivos entren en un ciclo interminable de bloqueo y reinicio que solo puede finalizar restaurándolos a su configuración de fábrica.

Aunque la compañía intentó mitigar el problema introduciendo un límite en la longitud del nombre que puede establecer una aplicación o el usuario, se descubrió que no hizo nada para evitar que un atacante ejecute una versión anterior que permite nombres de dispositivos excesivamente largos y luego hacer que la víctima acepte una invitación deshonesta por medio de un correo electrónico de phishing.

La solución se produce semanas luego de que el investigador de seguridad cibernética, Trevor Spiniolas, quien descubrió la vulnerabilidad, llamó a la empresa por *«no tomar el asunto en serio»* a pesar de haberlo informado en agosto de 2021 y dejar a sus clientes expuestos a un problema bastante grave.

> «La falta de transparencia de Apple no solo es frustrante para los investigadores de seguridad, que a menudo trabajan gratis, sino que también represente un riesgo para millones de personas que utilizan productos Apple en su vida cotidiana al reducir la responsabilidad de Apple en asuntos de seguridad», agregó Spiniolas.